Smishing 해킹에 대한 수사기술

문순호* · 박대우**

*,**호서대학교 벤처대학원

Invstigation about Sminshing Hacking

Soon-hol Moon* · Dea-Woo Park**

*,**Hoseo Graduate School of Venture

E-mail : nanmoonsh@naver.com · prof_pdw@naver.com

요 약

본 연구는 지능화되고 있는 Smishing 수사기술에 대해 연구한다. 최근 스마트폰 사용자가 늘어나고 있음에 따라 그 에 따른 Smishing 피해 또한 늘어났다. Smishing 위험은 스마트폰 사용자라면 항상 존재한다. 해커는 스마트폰에 있는 전화번호 개인정보, 스마트폰뱅킹, 소셜네트워크 서비스, 모바일 쇼핑, 공인인증서 등을 이용해 Smishing 공격으로 이익을 취득한다. 이 연구에서는 Smishing 사고가 국민의 안전한 사이버생활에 위협을 주고 있어 Smishing수사기술에 대한 연구가 필요하다.

ABSTRACT

This paper proposed have been the business card information to the computer when creating business card printing agency saved to a file, there is always the risk of personal information leakage. Application file organization information into the card, the name, phone number, email address information, such as is capable of easily accessible because it is not encrypted. This paper proposed it encrypts the information entered on the Business Card application file to automate the process of the card application and simplifying the business card application process minimizes the work of staff and linked directly to the print shop how to automatically delete the print file after the completion of business card printing and research.

키워드

Smishing, Investigation, Hacking Attack

Ⅰ. 서 론

2015년 9월 현재, 경찰청은 추석 명절이 다가오면서 추석택배 지연에 따른 배송조회, 추석인사 및 선물확인, 유명업체 이벤트교환권 등 다양한 사칭 문구의 스미싱 피해 발생이 우려됨에 따라 피해예방을 위해 홍보활동을 적극 추진하고 있다.

2014년 추석명절 전후2주간(“14.9.1~9.15) 사이버안전국에 접수된 스미싱 신고건수는 추석 전후 집중발생함에 따라 여전히 주의를 요한다[1].

최근 현대사회에 있어 범죄자들의 지능적이고 조직적이며, 다양하고 수단화 되고 있는 가운데 스미싱 또한 계속적으로 주의 깊게 예방해야 한다.

아래의 <표1>은 알약 이스트소프트가 2015년 상반기 스미싱현황을 나타낸 것이다.

여전히 비슷한 내용의 스미싱이 반복적으로 나타남을 알 수 있다.

따라서 본 논문에서는 지능화되고 있는 Smishing 수사기술에 대해 연구하고자 한다[2].

<표 1> 일약 안드로이드 2015년 상반기 스미싱현황

내용별 분류	소계(건)
결혼	23,967
입학	1,140
택배	1,013
훈련	655
선물	493
기타	39,112
총합	66,380

II. 관련연구

2.1 스미싱사고

스미싱(Smishing)은 문자메시지(SMS)와 피싱(Phishing)의 합성어다. 웹사이트링크가 포함된 주소를 사회공학적 방법과 노출되기 쉽게 문자메시지를 보내면 사용자는 문자메시지에 링크된 앱의 링크(URL:Uniform Resource Locator)를 클릭하고 트로이목마가 주입되어 사용자가 모르는 사이에 시용자의 개인정보나 공인인증서를 탈취하는 수법으로 휴대폰 해킹기법을 말한다. 범인에게 소액결제 인증번호 전송을 함으로써 사이버머니,게임아이템을 구입하게 되면 스마트폰 피해자의 소액결제 대금으로 청구되는 등 피해를 발생시킨다.[3]

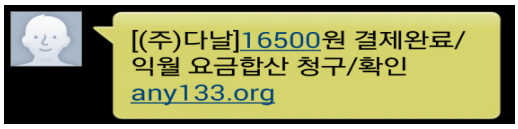

그림 1. 다날 소액결제 실제 스미싱문자

2.2 스미싱사고 신고

스미싱사고가 일어났을 경우 경찰청 사이버안전국의 "사이버범죄 신고시스템"이나 민간으로 불법스팸대응센터 118에 신고접수를 하면 된다. 신고처리절차는 사용자가 신고를 하고 신고가 접수되면 위법사실 확인 단계를 거쳐 검찰과 경찰이 수사를 하게 되고 법 위반의 정도에 따라 과태료를 물게되거나 경중에 따라 벌금과 징역벌을 질수 있다.

2.3 스미싱 수사기관

수사기관은 법률상 수사의 권한이 인정되어 있는 국가기관으로 수사기관에는 검사와 사법경찰관리가 있다.

스미싱은 사이버범죄로 국가 수사기관으로 경찰과 검찰의 사이버수사팀에 수사한다.

수사자는 일반적으로 범죄현장에서 일어나는 다른 모든 일을 조정할 책임을 가진다.

첫째 범죄현장을 담당하고 있는 수사자는 모든 사람에게 명령체계를 알려줘서 중요한 결정이 그를 통해 이뤄지도록 해야한다.

둘째 수색영장이 허용하는 범위에서 컴퓨터 하드웨어나 소트트웨어, 메모, 매뉴얼, 로그를 조사하는 범죄현장의 수색을 지시해야 한다.

셋째 사라지기 쉬운 증거를 보존하고, 디스크를 복제하고, 시스템을 끌 준비가 될 때까지 증거를 보호하는 증거의 무결성을 유지해야 한다[4].

III. Smishing해킹 침해사고 분석

3.1 Smishing 해킹

스미싱 해킹은 해커가 사용자에게 위조된 웹페이지의 링크(URL:Uniform Resource Locator)가 포함된 SMS를 보내 접속하게는 공격기법이다[5].

아래그림2은 그림1의 실제 주소를 웹페이지에서 입력해서 들어간 화면이다.

그림 2. 스미싱의 숨겨진 악성코드 파일

3.2 Smishing 침해사고 분석

침해사고란 해킹,컴퓨터바이러스,논리폭탄,메일폭탄,서비스 거부 또는 고출력 전자기파 등 방법으로 정보통신망 또는 이와 관련된 정보시스템을 공격하여 발생한 사고로 정의한다[6].

스미싱 침해사고가 발생시 정보가 유출되었는지와 어떤 정보가 유출되었는지, 시스템 피해규모와 범위에 대한 정보를 우선시 해야한다.

IV. Smishing 해킹에 대한 수사기술연구

4.1 모바일포렌식 상 수사기술

모바일포렌식은 최근 늘어나고 있는 스마트폰과 모든 휴대용 기기에 필요한 정보를 추출하여 분석하는 포렌식 분야를 말한다.

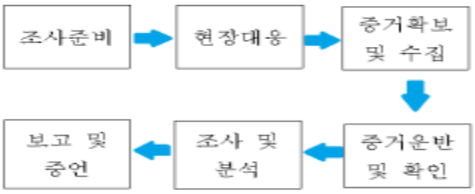

그림 3. 모바일포렌식 조사모델

스미싱은 스마트폰에서 이루어지는 대표적인 모바일 범죄이다. 일반수사절차와 다르지 않게 범죄수사절차에 따라 수사계획을 세우고 현장에

나가 환경을 보존하고 증거물을 절차에 따라 수집하고 분석하고 사건보고서를 작성한다[7].

스미싱 수사도 모바일포렌식 조사모델처럼 그림3과 비슷하지만 관계기관이나 사건의 특성에 따라 약간 상이할 수 있다.

4.2 Smishing 해킹에 대한 수사기술

스미싱 해킹은 모바일 포렌식의 분야로 Mobile Forensic 분석도구인 Oxygen2014 suit와 자바 decompiler을 통해 분석하였다.

Smishing해킹에 감염되면 스마트폰 개인정보, 연락처, 문자메시지, 통화기록, 달력 등을 통해 수사분석을 한다.

안드로이드 문자메시지 정보는 mmssms.db라는 DB name에 그에 따른 Table 13종류, 99개의 Field와 Type이 정보를 나타내준다.

message라는 Table에 adress와 text등을 조사하면 메시지를 보낸사람과 문자메시지 내용을 취득할 수 있다[8].

Ⅴ. 결론 및 향후연구

본 논문은 스미싱에 대한 국내피해사례와 증가하고 있는 스미싱해킹에 대해 수사기술로 분석하였다. 해커들은 날로 진화하고 있으며 그에 따라 모바일 포렌식 수사에 있어 스미싱해킹 수사기술은 갈수록 중요해지고 있다.

향 후 연구로는 모바일 포렌식 분야의 수사지침과 스마트폰 포렌식으로 분석하는 해킹에 대해 연구하여야 할 것이다.

참고문헌

[1] http://cyberbureau.police.go.kr/board/boardView.do?board_id=news&id=5459&page=1&mid=020100, 경찰청 사이버안전국 홍보자료

[2] http://blog.alyac.co.kr/406,알약블로그

[3] http://kin.naver.com/open100/detail.nhn?d1id=1&dirId=10702&docId=1433420&qb=7Iqk66+47IuxIOusuOyekOuPme2WpQ==&enc=utf8&section=kin&rank=1&ssssst0-386218&sid=480UnzaxMQzvDZDcevljSA%3Dearch_sort=0&spq=0&pid=SQJfIdoRR1Gssv/ualCss%3D, 네이버 오픈백과 정의

[4] 사이버범죄 소탕작전 컴퓨터 포렌식 핸드북554p

[5] Joonhyouk Jang, Seunghwan Han, “Survey of Security Threats and Contermeasures on Android Enviornment", Vol11, No1(2014) pp01-12

[6] 정보통신망 이용촉진 및 정보보호 등에 관한법률 제2조 7항

[7] Heum park, “Cyber forensics domain ontology for cyber criminal investigation”, The Korea Institute of Information and Communication Engineering, Vol13, no8. 1687-1692,2009.08

[8] Dea-Woo Park, "Analysis on Mobile Forensic of Smishing Hacking Attack", The Korea Institute of Information and Communication Engineering, vol18, no2. 2878-2884, 2014.12